DIRECTORATE OF INFORMATION MANAGEMENT

Information Assurance Division (IAD)

Mr. Jim Preston, CISSP
Chuck Clark
Henry Felch
Ray Hand
Patty Harden
Gwen Phillips
Mark Saunders
Cindy Thornburg

DIRECTORATE OF INFORMATION MANAGEMENT

CURRENT ISSUES

- Adobe Reader Vulnerability and Method to Patch (upgrade to v7.0.2)

- CDROM Write Issue with AGM III Image (Army Gold Master)

  It is a setting in the local policy. We fixed it on the NIPR image by editing the registry:

  [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon]

  "allocatecdroms"="0"

  The default setting is ‘Enabled’ in the AGM III RIS Image.

DIRECTORATE OF INFORMATION MANAGEMENT

CURRENT ISSUES -cont-

- HP Digital Sender Model 9200

  Not secure on the network.

- Multi-Function Printers Are Actually Digital Senders
- Email Phishing

  Purportedly from Armed Forces Bank.

  Attempting identity theft for financial gain.

Information Assurance Mission Statement

- ***Our sole mission is to protect and defend network availability, protect data integrity, and provide the ability to implement effective computer network defense for the Fort Carson Network.***

DIRECTORATE OF INFORMATION MANAGEMENT

Information Assurance (IA)

- IA (U.S. Definition)

  Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection and reaction capabilities.

  Protect - Provides for the availability, integrity, authenticity, confidentiality, and non-repudiation of information or transactions

  Detect - Provides for the ability to detect efforts to disrupt and deny services

  React - Provides for reconstitution of information and services in case of a successful disruption or denial

Information Assurance (IA) Definitions

- **Availability** - Information and information systems are available when needed to support mission critical, mission support, and administrative purposes.
- **Integrity** - Data is unchanged from its source--has not been accidentally or maliciously altered.
- **Authentication** - Data, and their originators, are authentic, and that a recipient is eligible to receive specific categories of information
- **Non-Repudiation** - Strong and substantial evidence of an information exchange or transaction.
- **Confidentiality** - Information can be read only by authorized entities e.g. encryption

Information Assurance Punitive aspects of AR 25-2

- In the event that any Commander or supervisor intends to take adverse administrative action against any employee (U.S. service member, civilian, LN), they should consult with their assigned legal representation or the JAG office prior to taking such action.

Information Assurance
AR 25-2

- AR 25-2, paragraph 1-1 j makes various provisions of AR 25-2 punitive in nature.
- Military could be subject to Article 92 of the UCMJ.
- DA Civilians subject to administrative punishment
- Contractors subject to contract remedies.

DIRECTORATE OF INFORMATION MANAGEMENT

Information Assurance
AR 25-2 Prohibitions

- Paragraphs 3-2 and 3-3. Failure to perform the listed duties if assigned to listed position.
- Paragraph 4-6. Failure to comply with software security controls. (e.g. violating baselines or using shareware/freeware)
- Paragraph 4-7. Failure to comply with database management directives and controls. (e.g. unauthorized access)
- Paragraph 4-10. Failure to comply with personnel access restrictions. (e.g. use of maintenance personnel or use of data recovery services)

DIRECTORATE OF INFORMATION MANAGEMENT

Information Assurance
AR 25-2 Prohibitions

- Paragraph 4-11. Failure to comply with security safeguards. (e.g physical security)
- Paragraph 4-12. Failure to comply with password controls.
- Paragraph 4-13. Improper release of information concerning information system infrastructure architecture. (e.g public access to FOUO material)
- Paragraph 4-16. Failure to comply with information systems media protection requirements. (e.g. protect classified material)

DIRECTORATE OF INFORMATION MANAGEMENT

Information Assurance
AR 25-2 Prohibitions

- Paragraph 4-17. Failure to comply with classification labeling and marking requirements.
- Paragraph 4-18. Failure to properly clear, purge, destroy, sanitize, or otherwise dispose of media.
- Paragraph 4-20. Failure to comply with network security requirements. (e.g. use of commercial networks, forward of official mail to civilian email systems)
- Paragraphs 4-21and 4-22. Failure to comply with incident and intrusion reporting requirements.

DIRECTORATE OF INFORMATION MANAGEMENT

Information Assurance
AR 25-2 Prohibitions

- Paragraph 4-23. Failure to comply with requirements concerning compromised systems.
- Paragraph 4-25. Failure to follow IAVA compliance reporting requirements.
- Paragraph 4-30. Violations of restrictions on employee and contractor owned information systems.
- Paragraph 6-1. Failure to comply with COMSEC requirements.

Information Assurance
AR 25-2 Prohibitions

- Paragraph 6-2. Violation of the restrictions on protected distribution systems. (e.g inspection of and access to secure network boxes/pipes in unclassified areas)
- Paragraph 6-5. Violations of restrictions on telecommunications devices. (e.g. government or personal PDA's, cell phones, pagers, etc in secure areas)

DIRECTORATE OF INFORMATION MANAGEMENT

COMPUTER NETWORK DEFENSE

- Network Security
- Policy and Procedures
- Inspection and Compliance
- Training and Assistance
- SIPRNet and NIPRNet Accreditations
- Software Accreditations
- Initial Incident Investigation
- Spillage Containment

5 Classes of Attacks

1) **Passive**.

Passive attacks include traffic analysis, monitoring of unprotected communications, decrypting weakly encrypted traffic, and capture of authentication information (e.g., passwords).

Passive intercept of network operations can give adversaries indications and warnings of impending actions.

Passive attacks can result in disclosure of information or data files to an attacker without the consent or knowledge of the user.

Examples include the disclosure of personal information such as credit card numbers and medical files.

5 Classes of Attacks -cont-

2) **Active**.

Active attacks include attempts to circumvent or break protection features, introduce malicious code, or steal or modify information.

These attacks may be mounted against a network backbone, exploit information in transit, electronically penetrate an enclave, or attack an authorized remote user during an attempt to connect to an enclave.

Active attacks can result in the disclosure or dissemination of data files, ***denial of service*** (DoS or DDoS), or modification of data.

Denial of Service (DoS) & Distributed Denial of Service (DDoS)

- In addition to the tools specifically crafted to execute DoS and DDoS attacks, some compromised systems that run some of the more recent widely used tools use Instant Messenger (IM) and Peer to Peer (P2P) file sharing applications as agents to perform the attack.

5 Classes of Attacks -cont-

3) **Close-in**.

Close-in attack consists of regular type individuals attaining close physical proximity to networks, systems, or facilities for the purpose of modifying, gathering, or denying access to information.

Close physical proximity is achieved through surreptitious entry, open access, or both.

5 Classes of Attacks -cont-

4) **Insider**.

Insider attacks can be malicious or non-malicious.

Malicious insiders intentionally eavesdrop, steal or damage information, use information in a fraudulent manner, or deny access to other authorized users.

Non-malicious attacks typically result from carelessness, lack of knowledge, or intentional circumvention of security for such reasons as getting the job done.

5 Classes of Attacks -cont-

5) **Distribution**.

Distribution attacks focus on the malicious modification of hardware or software at the factory or during distribution.

These attacks can introduce malicious code into a product, such as a back door to gain unauthorized access to information or a system function at a later date.

DIRECTORATE OF INFORMATION MANAGEMENT

NETWORK BASED TOOLS

- Firewall
- Intrusion Detection System (IDS)
- Internet Filters & Virus Wall
- Vulnerability Scanning
- Traffic Monitoring

FIREWALL METHODOLOGY

- The primary function of a firewall is to control the access to and from a protected network. Packets attempting to pass through the firewall will be examined and evaluated to determine whether or not access is allowed based on the established rules.

- NOTE: Although the use of a firewall greatly increases ones security posture, having a firewall does not necessarily guarantee absolute protection of a network, or the systems on the network.

FIREWALL METHODOLOGY

- Default is to deny access to all
- Pass is by exception and requires a firewall rule
- Firewall rule requests go through IA for approval

Intrusion Detection (IDS)

- 7 Sensors monitor all network traffic
  - External above the firewall
  - DMZ traffic
  - Internal below the firewall
  - Server farm area (3 sensors)
  - Pueblo

- All events logged and reviewed; emails sent for specific events

Vulnerability Scans

- **ISS System Scanner**
  - Requires Agent On Each Computer
  - Servers Only
- **ISS Internet Scanner**
  - Requires only a connection to the network
  - Identification of network assets
  - Identify/Verify vulnerabilities
- **Harris STAT Scanner**
  - Requires Local Admin Rights
  - IAVA Compliance for AVTR
- **Retina eEye**
  - Identification of network assets
  - Port Scans
  - IAVA Compliance

DIRECTORATE OF INFORMATION MANAGEMENT

IAVA

- Information Assurance Vulnerability Alert
- Issued by CIO-G6/ACERT, G3 DISOPS
- Mandatory Compliance
- IAVA Message contains:
  - Vulnerability and description of problem
  - Specific actions and suspense for compliance
- ACERT must approve any extensions
- https://www.acert.1stiocmd.army.mil

DIRECTORATE OF INFORMATION MANAGEMENT

Asset and Vulnerability Tracking Resources

- A&VTR is a database to gather and consolidate IAVA reporting and training
- All assets must be registered in A&VTR
- Assign primary and alternate POC for each asset
- Assets have been entered using HARRIS Stat
- DOD and Army Policy – IAVA Compliance is a force protection issue
- Command responsibility to report and comply with IAVAs – mandatory
- Located at https://newia.us.army.mil/modules
- Uses IAO login. May request one at the above site.

BLOCKING PORTS

- Ports on switches will be blocked for the following reasons:
  - Peer-to-Peer software
  - Spyware
  - Virus infections
  - IAVA non-compliance
  - Unauthorized computers (Personal computers, E-Army computers, etc)
  - IDS incidents
  - Incorrect or old naming conventions

DIRECTORATE OF INFORMATION MANAGEMENT

WHAT CAN YOU DO AS IMO’s

- Work on any IAVAs that you receive from our scans
- Educate users about P2P software, spyware and consequences
- Personal computers and E-Army-U computers: If you find them - get them off the network
- Messages that pop-up on the screen need to be relayed to the IMO
- Maintain a list of computers, where they are located, and any port information that you can identify
- If a computer is required to come into IA for investigation, bring to us ASAP.

Unauthorized Operating Systems

- Windows 9X, ME, 3.11
- UNIX/LINUX Workstations
- Windows 2000 by Exception
- NT4 according to below:
  - June 30 2004 for NT4 Workstations
  - June 30 2005 for NT4 Servers

Unauthorized Application Software

- Outlook 3rd Party Add-ons
- Messenger/Chat (AR 25-2)
- P2P/Distributed Computing
- Personal Firewalls
- Port Scanner/Blockers
- Freeware/Shareware
- ANY non-Army Approved Software

THREAT MITIGATION

- Peer to Peer Software
- Spyware (Adware)
- Spam

PEER TO PEER SOFTWARE

- Winmx, Morpheous, BearShare, Limewire, Kazaa, Napster (even the “legal” version), etc. etc. etc…
- All P2P software contains Spyware
- Copyright infringement violations can cost the Army millions of dollars
- Prohibited by Army Directive.

DIRECTORATE OF INFORMATION MANAGEMENT

PEER TO PEER SOFTWARE SEEN ON THE NETWORK

Ares, AudioGalaxy, AresLite, AudioGnome, BadBlue, BearShare, BitTorrent (btdownloadgui.exe), Blubster, BoDeTeLLa, DC++, Directconnect, EarthStation5 (es5.exe), eDonkey, eMule, eMule+, Filetopia, FolderShare, Freenet, Freewire, Gnucleus, Gnutella, Grokster, iMesh, Joltid (P2P Networking.exe), Kazaa, Kazaa lite (kpp.exe), Kazoom, Limewire, LordofSearch, MLDonkey (mlnet.exe), Morpheus, MP2P, Mute (fileSharingMUTE.exe), MyNapster, Napigator, OneMX, Opera (oDC.exe), Overnet, Phex, Piolet, RockItNet, Seti@home, Shareaza, Soulseek(slsk.exe), Swaptor, Tripnosis, TrustyFiles, WarezP2P, Waste, WinMX, WrapsteR, XoLoX, Zpoc

DIRECTORATE OF INFORMATION MANAGEMENT

SPYWARE (ADWARE)

- All Adware is Spyware
- 25,542 variants in the wild as of Mar 05
- Downloaded through Inet drive-by's, clicking on pop ups, porn and music sites, browsing any non-traditional sites
- At minimum, captures browsing habits and reports back to owner
- At worse, installs keystroke loggers capturing passwords, etc. and sends back to owner

DIRECTORATE OF INFORMATION MANAGEMENT

SPAM EMAIL

- Nothing you can do about it at this time.
- There are top level and policy solutions out there. Top level equals big $$$, policy ruffles too many feathers.
- Generated from legitimate user computers as well as “spoofed” IP addresses.
- Contains links to porn, spyware downloads, phishing schemes. Most URL’s in spam email are active for only a few hours.
- Much of it is from China.

DIRECTORATE OF INFORMATION MANAGEMENT

Wireless

- 802.11x – Army, DoD, NSA Approved Gear
- Blackberry – Commander Approval
- Wireless Networks Require IA Approval and Accreditation

There is a viable, secure and cost efficient solution to your wireless needs.

HANDLING POTENTIAL COMPUTER COMPROMISES

- **Call and / or assign any IA related work tickets to us via Remedy ASAP**
- **IA related incidents include Spillage, Spyware, Peer to Peer software, spam, virus activity, wireless requests, inappropriate usage (porn, etc.), personal computers on network, and other potential compromises**
- **Be very careful when working in a machine so as not to disturb potential evidence**
- **Should inappropriate content or usage be suspected on a machine, logoff immediately and *unplug network cable*. DO NOT TURN OFF MACHINE.**

DIRECTORATE OF INFORMATION MANAGEMENT

SIPRNET E-Mail Requests

- NIPRNET vs. SIPRNET
- Two Types of SIPRNET – Local vs. AKO-S
- Requirements:
  + Ft Carson Form 1001-E (FC 1001-E) dated Oct 2004 or later
  + NATO Briefing date posted on FC 1001-E
  + Local Records Check (LRC)(FC-18E) at PMO (within last 30 days)
  + DCII/JPAS printout (within last 30 days)
- 3-5 working days to process request
- Valid for 1 year
- Accounts may be denied if any derogatory info is found doing LRC
- Final approval rests with the Ft Carson IAM

Inspection Program

- Formal:
  - Security Manager Inspection
  - Command Inspection
  - IG Quick Look

- Informal – Unit assistance

Initial Incident Reporting

- IMO Responsibility:
  - Recognize a problem
  - Secure the computer properly – leave powered on
  - Notify DOIM Information Assurance
- IA Responsibility:
  - Decide level of involvement:
    + Criminal Investigation Division
    + Military Intelligence
    + Commander
- Spillage

DIRECTORATE OF INFORMATION MANAGEMENT

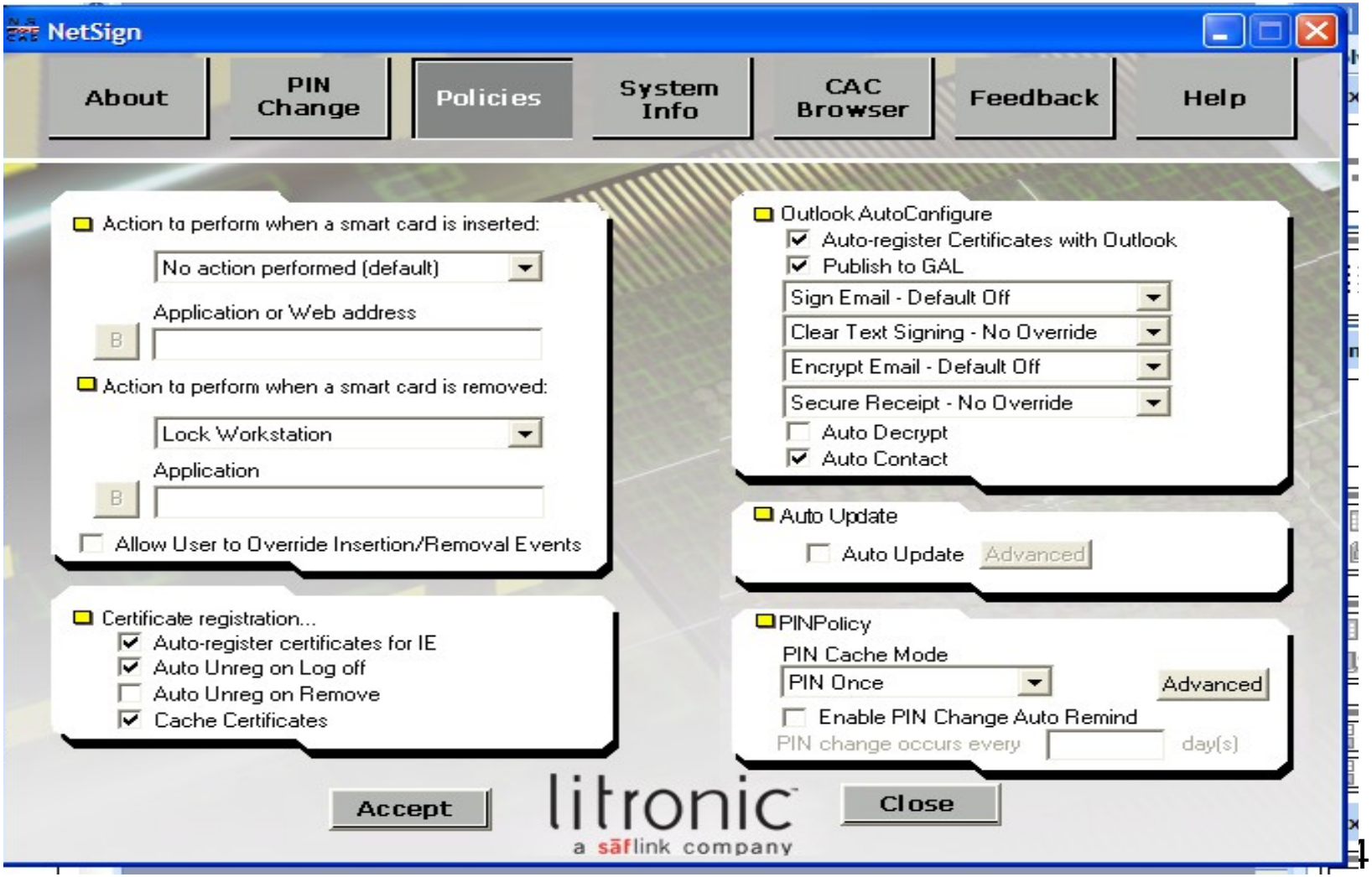
CAC / PKI

- Netsign 4.2.0.206
- GWOT information must be digitally signed and encrypted
- Publish certificates to the GAL
- Expiring Certificates
- Pin Reset
- https://setdweb.setd.army.mil/

Auto Contact

- Default Setting: Enable Auto Contact in Netsign
- Benefit to End Users: Automatically saves the Contact
- Provides extra security: Warns if contact has multiple certficates.

DIRECTORATE OF INFORMATION MANAGEMENT



Accreditation

- All networks and their computers will be accredited before they are placed on the network (AR 25-2)
- Accreditations are good for 3 years unless there is a major change; Reason, because the change can cause vulnerability:
  - Hardware (new equipment or upgrade)
  - Software (new programs or operating system)
  - New “key” personnel such as the IASO or IMO

Accreditation

- The accreditation is the System Security Authorization Agreement (SSAA) and Appendix
- The SSAA covers non-changing items such as process to use the computer, mission of the organization, mission and use of the computer
- The Appendix contains where the computers are and how they are set up. Also, the unit SOP and User Agreement
- Templates can be downloaded from http://www.carson.army.mil/doim/ia , click on ‘ Carson users only IA pages’, Accreditations (DITSCAP), and SSSA template and sample appendices.

DIRECTORATE OF INFORMATION MANAGEMENT

Information Assurance Division

• Jim Preston	526-0565
• Chuck Clark	526-5510
• Henry Felch	526-8985
• Ray Hand	526-3965
• Patty Harden	524-4541
• Gwen Phillips	526-4596
• Mark Saunders	524-0588
• Cindy Thornburg	526-1386

IA Website on the Internet
http://www.carson.army.mil/doim/ia